A.R.T.
International
SERVICE - TRADUCTION - INTERPRETATION

TRANSLATOR'S CERTIFICATE

I, **Mr. DERISSON,**

of A.R.T. International – 85, rue Galliéni 95170 Deuil-la-Barre, France

declares as follows:

1. That I am well acquainted with both the English and French languages, and

2. That the attached document is a true and correct translation made by me to the best of my knowledge and belief of :

PATENT APPLICATION N° W0 00/50977 (PCT/FR00/00472)

Dated this 14th day of August 2001

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"EXPRESS MAIL" MAILING LABEL NUMBER EL747089419US

DATE OF DEPOSIT August 24, 2001

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231

Greg French

(TYPED OR PRINTED NAME OF PERSON MAILING PAPER OR FEE)

(SIGNATURE OF PERSON MAILING PAPER OR FEE)

THIS PAGE BLANK (USPTO)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 01 novembre 2000 (01.11.00)	
Demande internationale no PCT/FR00/00472	**Référence du dossier du déposant ou du mandataire** 014415
Date du dépôt international (jour/mois/année) 25 février 2000 (25.02.00)	**Date de priorité** (jour/mois/année) 25 février 1999 (25.02.99)
Déposant ROMAIN, Fabrice	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

25 septembre 2000 (25.09.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Diana Nissen

no de téléphone: (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

BALLOT, Paul
Cabinet Ballot
7, rue Le Sueur
F-75116 Paris
FRANCE

Date d'expédition (jour/mois/année)
09 octobre 2001 (09.10.01)

Référence du dossier du déposant ou du mandataire
014415

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR00/00472

Date du dépôt international (jour/mois/année)
25 février 2000 (25.02.00)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☐ le déposant ☐ l'inventeur ☒ le mandataire ☐ le représentant commun

Nom et adresse

BALLOT, Paul
Cabinet Ballot-Schmit
7, rue Le Sueur
F-75116 Paris
FRANCE

RECEIVED
OCT 31 2001
Group 2100

Nationalité (nom de l'Etat):

Domicile (nom de l'Etat):

no de téléphone
01 40 67 11 99

no de télécopieur
01 45 01 98 28

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☐ la personne ☒ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse

BALLOT, Paul
Cabinet Ballot
7, rue Le Sueur
F-75116 Paris
FRANCE

Nationalité (nom de l'Etat):

Domicile (nom de l'Etat):

no de téléphone
01 40 67 11 99

no de télécopieur
01 45 01 98 28

no de téléimprimeur

3. Observations complémentaires, le cas échéant:
Changement de dénomination sociale du mandataire.

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☒ à l'administration chargée de l'examen préliminaire international
☐ aux offices désignés concernés
☒ aux offices élus concernés
☐ autre destinataire:

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:
Philippe Bécamel

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 09 octobre 2001 (09.10.01)	
Demande internationale no PCT/FR00/00472	**Référence du dossier du déposant ou du mandataire** 014415
Date du dépôt international (jour/mois/année) 25 février 2000 (25.02.00)	**Date de priorité** (jour/mois/année) 25 février 1999 (25.02.99)
Déposant ROMAIN, Fabrice	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

25 septembre 2000 (25.09.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Philippe Bécamel

no de téléphone: (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 014415	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 00472	Date du dépôt international *(jour/mois/année)* 25/02/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 25/02/1999
Déposant STMICROELECTRONICS S.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [X] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted]

Demande internationale No
PCT/FR 00/00472

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 septembre 1997 (1997-09-12) abrégé page 1, ligne 1 -page 2, ligne 21 page 3, ligne 11 - ligne 29	1,4,5
Y	---	6
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 septembre 1991 (1991-09-25) colonne 1, ligne 1 -colonne 3, ligne 1 colonne 6, ligne 38 - ligne 52	1,5
A	---	2
Y	GB 2 319 705 A (MOTOROLA LTD) 27 mai 1998 (1998-05-27) abrégé; figure 1 page 3, ligne 8 - ligne 13 revendications 1-8	6

	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 juin 2000	19/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no. 6, page 565-584 XP000415701 ISSN: 0167-4048 page 568, colonne de gauche, alinéa 3 -page 569, colonne de droite, alinéa 2 page 570, colonne de droite, alinéa 3 page 571, colonne de droite, alinéa 3 -page 572, colonne de gauche, alinéa 2 ---	2,3
A	DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6 octobre 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731 page 78 -----	2

1

INTERNATIONAL SEARCH REPORT

Information patent family members

International Application No
PCT/FR 00/00472

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9733217 A	12-09-1997	FR 2745924 A	12-09-1997
		AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
GB 2319705 A	27-05-1998	WO 9822878 A	28-05-1998
		EP 0938707 A	01-09-1999

09/914172

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 014415	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/00472	Date du dépot international *(jour/mois/année)* 25/02/2000	Date de priorité *(jour/mois/année)* 25/02/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F1/00		
Déposant STMICROELECTRONICS S.A. et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
25/09/2000	22.05.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Dixon-Hundertpfund K N° de téléphone +49 89 2399 2857

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00472

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

   Description, pages:

   1-7 version initiale

   Revendications, N°:

   1-6 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, n^{os} :

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-6 (oui)
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-6 (non)
Possibilité d'application industrielle	Oui :	Revendications	1-6 (oui)
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

V. Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

1. Il est fait référence aux documents suivants:

D1: WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 septembre 1997 (1997-09-12)
D2:EP 0 448 262 A (GEN INSTRUMENT CORP) 25 septembre 1991 (1991-09-25)
D3: GB 2 319 705 A (MOTOROLA LTD) 27 mai 1998 (1998-05-27)
D4: COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no. 6, page 565-584 XP000415701 ISSN: 0167-4048
D5: DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6 octobre 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731

2. L'objet des revendications indépendantes 1, 5 et 6 diffère de ce qui est connu du document D1 (voir en particulier page 1, ligne 6 à la page 3, ligne 29), qui est considéré comme étant l'état de la technique le plus proche, en ce que:

(i) les opérations factices sont de même type que les opérations utiles (revendications 1, 5, 6),
(ii) le dispositif électronique d'exécution de l'algorithme est compris dans une carte à puce (revendication 6).

Les différences (i) et (ii) sont simplement chacune une des possibilités parmi plusieurs entre lesquelles l'homme du métier pourrait choisir, selon le cas d'espèce, sans qu'une activité inventive soit impliquée (Article 33(3) PCT). Par exemple, la différence (i) est connue de D4 ou de D5 et de comprendre un dispositif électronique d'exécution de l'algorithme dans une carte à puce est connu de D3.

3. Les revendications dépendantes 2 à 4 ne contiennent aucune caractéristique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences du PCT en ce qui concerne l'activité inventive, car les caractéristiques sont ou connues de D1 ou elles sont seulement l'une des possibilités, que la personne du métier pourrait choisir parmi des plusieurs possibilités immédiates, selon le cas d'espèce.

VII. Irrégularités dans la demande internationale

1.1 D2 décrit un procédé de sécurisation qui comprend les étapes d'exécuter une ou plusieurs routines intérims avant l'occurrence d'un événement observable a l'extérieur et l'exécution d'une routine prédéterminée et l'étape de varier de façon aléatoire la durée des routines intérims.

D4 décrit plusieurs procédés de sécurisation dont un est d'introduire une ou plusieurs opérations factices dans un enchaînement d'opérations.

D5 décrit un microcontrolleur qui est sécurisé en comprenant dans un cycle d'instruction deux accès mémoire dont un est toujours factice, l'ordre entre les accès mémoire vrais et factices étant déterminé de manière aléatoire.

1.2 Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D1, D2, D3, D4 et D5 et ne cite pas ces documents.

La description ne cite pas de document reflétant l'état de la technique décrit à la page 1, ligne 23 à la page 3, ligne 31 (règle 5.1 a) ii) PCT).

Translation
09/914192

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 014415	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00472	International filing date (*day/month/year*) 25 February 2000 (25.02.00)	Priority date (*day/month/year*) 25 February 1999 (25.02.99)
International Patent Classification (IPC) or national classification and IPC G06F 1/00		
Applicant STMICROELECTRONICS S.A.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
25 September 2000 (25.09.00)	22 May 2001 (22.05.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00472

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-7, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:

pages 1-6, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the drawings:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 00/00472

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-6	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-6	NO
Industrial applicability (IA)	Claims	1-6	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: WO 97 33217 A (UGON MICHEL; BULL CP8 (FR)) 12 September 1997 (1997-09-12)

D2: EP 0 448 262 A (GEN INSTRUMENT CORP) 25 September 1991 (1991-09-25)

D3: GB 2 319 705 A (MOTOROLA LTD) 27 May 1998 (1998-05-27)

D4: COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAMME EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, NL, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no 6, pages 565-584 XP000415701 ISSN: 0167-4048

D5: DALLAS SEMICONDUCTOR CORP: "SECTION 1: INTRODUCTION" 6 October 1993 (1993-10-06), DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3, 7, 8, 73, 77-80, 82, 152-156, 229, 290-292 XP002053731.

2. The subject matter of independent Claims 1-5 and 6 differs from that of document D1 (see in particular page 1, lines 6 to page 3, line 29), which is considered the closest prior art, in that:

(i) the dummy operations are of the same type as the working ones (Claims 1, 5, 6),

(ii) the electronic device for executing the algorithm is contained in the smart card (Claim 6).

The differences (i) and (ii) are simply one of several possibilities that a person skilled in the art might select, according to the circumstances, without thereby being inventive (PCT Article 33(3)). For example, the difference (i) is known from D4 or D5, and the incorporation of an electronic device for executing an algorithm in the smart card is known from D3.

3. Dependent Claims 2-4 do not contain any feature which, in combination with those of any one of the claims to which they refer, defines subject matter that meets the PCT requirements of inventive step, since said features are either known from D1, or are simply one of several obvious possibilities that a person skilled in the art might select, according to the circumstances.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1.1. D2 describes a secure data processing method that includes the steps of executing one or more interim routines prior to the occurrence of an observable external event and executing a predetermined routine, and the step of randomly varying the duration of the interim routines.

D4 describes a plurality of secure processing methods, including that of incorporating one or more dummy operations in a chain of operations.

D5 describes a microcontroller that is rendered secure by including, in an instruction cycle, two memory accesses, one of which is always a dummy access, wherein the order of the real and dummy memory accesses is determined randomly.

1.2 Contrary to the requirements of PCT Rule 5.1(a)(ii), the description does not outline the relevant prior art set forth in documents D1, D2, D3, D4 and D5 and does not cite these documents.

The description does not cite any document describing the prior art mentioned on page 1, line 23 to page 3, line 31 (PCT Rule 5.1(a)(ii)).

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G06F 1/00 — A1

(11) Numéro de publication internationale: **WO 00/50977**

(43) Date de publication internationale: 31 août 2000 (31.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00472

(22) Date de dépôt international: 25 février 2000 (25.02.00)

(30) Données relatives à la priorité:
99/02364 25 février 1999 (25.02.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: STMICROELECTRONICS S.A. [FR/FR]; 7, avenue Galliéni, F–94250 Gentilly (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: ROMAIN, Fabrice [FR/FR]; Les Héliades Bâtiment A, 535, avenue de Bagatelle, F–13090 Aix–en–Provence (FR).

(74) Mandataire: BALLOT, Paul; Cabinet Ballot–Schmit, 7, rue Le Sueur, F–75116 Paris (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: METHOD FOR MAKING SECURE A SEQUENCE OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT IN THE EXECUTION OF AN ALGORITHM

(54) Titre: PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME

(57) Abstract

The invention concerns a method for making secure a sequence of working operations, of the same type, performed by an electronic circuit in the execution of an algorithm. The method is characterised in that it comprises a step which consists in introducing randomly one or several dummy operations in the sequence of operations, so as to prevent fraudulent access, by statistical analysis of electric currents, to protected data.

(57) Abrégé

L'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Le procédé selon l'invention fait intervenir une étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices dans l'enchaînement d'opérations, afin d'empêcher un accès frauduleux, par une analyse statistique de courants électriques, à des données protégées.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME

La présente invention se rapporte à un procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Plus particulièrement, l'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, la sécurisation étant apportée par la présence d'informations parasites qui gênent l'observation, depuis l'extérieur du circuit électronique, des manifestations physiques associées à l'exécution des opérations utiles.

Dans le cadre de l'invention, un algorithme doit être compris en tant qu'enchaînement d'actions nécessaires à l'accomplissement d'une tâche. Il ne s'agit par conséquent pas nécessairement de la mise en oeuvre d'un programme informatique.

Le domaine d'application de l'invention est essentiellement le domaine de la cryptologie. La cryptologie peut se définir comme étant la science de la dissimulation de l'information. Elle constitue, avec la sécurité physique des composants et des systèmes d'exploitation, la dimension essentielle de la sécurité des cartes à puces. La cryptologie englobe la cryptographie, qui est l'art de chiffrer et de déchiffrer des messages, et la cryptanalyse, qui est l'art de casser les codes secrets.

Dans les cartes à puce, la cryptographie met en oeuvre divers mécanismes qui ont pour but d'assurer soit la confidentialité des informations, soit

l'authentification des cartes ou des utilisateurs, soit encore la signature des messages.

L'ensemble des moyens mettant en oeuvre la cryptographie forme un crypto-système. De tels crypto-systèmes renferment des informations confidentielles, notamment pour chiffrer et déchiffrer des messages numériques.

Parmi ces informations confidentielles, on peut citer les clés de chiffrement et de déchiffrement, qui sont des paramètres d'une convention secrète utilisée pour le chiffrement et le déchiffrement de messages numériques.

L'utilisation de ces clés de chiffrement et de déchiffrement nécessite souvent plusieurs transferts des données les caractérisant. Lors de leur utilisation au sein d'un crypto-système, les données caractéristiques de clés numériques et d'autres informations confidentielles circulent entre différents registres et modules de mémoire ou de traitement. Ces transferts entre registres et/ou modules se traduisent par l'apparition de courants électriques ou de champs magnétiques porteurs d'informations confidentielles. Les informations confidentielles peuvent, par exemple, concerner des clés de chiffrement et de déchiffrement.

De tels crypto-systèmes posent un problème de visibilité depuis le monde extérieur. En effet, une mesure des signaux électriques ou des champs magnétiques nés des échanges d'informations entre différentes parties du circuit peut permettre d'accéder à des informations confidentielles qui participent à la protection de données par le système de chiffrement ou de déchiffrement.

Par exemple, un des signaux électriques peut se situer au niveau du plot d'alimentation du circuit, que ce dernier soit interne ou externe.

En effet, au moment de l'utilisation de la clé numérique par un composant habilité tel qu'une carte à puce, une certaine visibilité, par exemple sur la clé numérique, est rendue possible par l'étude de tels signaux électriques. Les signaux électriques sensibles peuvent être observés sur différents plots du circuit reliant notamment différents registres ou modules de mémoire ou de traitement.

Une clé numérique peut ainsi être découverte suite à une accumulation de mesures de signaux électriques ou magnétiques et à une étude statistique de ces mesures.

D'une façon plus générale, tout circuit électronique a une consommation électrique liée aux opérations qu'il effectue. Il est possible, en mesurant cette consommation, de découvrir des informations cachées dans le circuit. Ce problème se pose en tout composant sécurisé, et notamment les composants pour cartes à puce.

La découverte de données protégées par observation de courant nécessite en général une reproductibilité de la mesure de courant afin d'effectuer les traitements statistiques.

Ainsi, lorsqu'un circuit électronique exécute un algorithme contenant des opérations identiques ou voisines, et répétitives, telles que des transferts de données confidentielles entre registres, et où l'observation fine des opérations une par une peut révéler une information confidentielle, une analyse statistique fondée sur la mesure des courants électriques précédemment cités peut nuire à la sécurité du circuit électronique.

La présente invention a pour objet de pallier les problèmes qui viennent d'être décrits.

L'invention propose donc une méthode permettant de parer à une divulgation, par observation du courant, de données protégées.

A cet effet, l'invention propose un procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme qui assure la non-visibilité vis-à-vis d'une analyse des signaux électriques lors des transferts de données entre différents registres.

Pour atteindre ces objectifs, l'invention propose d'insérer des opérations factices dans un enchaînement d'opérations utiles, de même type, effectuées dans le cadre de l'exécution d'un algorithme. Les opérations factices sont très ressemblantes aux opérations utiles. Chaque opération factice est insérée à un rang aléatoire pour chaque exécution de l'algorithme. Ainsi, l'acquisition de mesures de courant comparables devient très difficile.

Une opération factice peut être conçue comme une opération présentant une signature identique ou très proche en pratique d'une opération utile en termes de paramètres physiques observables associés à l'exécution de cette instruction (consommation de courant, rayonnement magnétique, etc.). Ces paramètres physiques peuvent être notamment détectés au niveau d'un terminal d'alimentation en courant ou en tension du circuit.

De la sorte, les présentes opérations factices ne peuvent pas être détectées échantillon par échantillon, et donc empêchent ou du moins rendent très difficile une analyse statistique.

L'invention concerne donc un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des

opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations utiles.

Une opération factice du même type qu'une opération utile peut prendre différentes formes selon l'application en cours, dès lors qu'elle présente des caractéristiques physiques qui apparaissent identiques ou suffisamment proches d'une opération utile pour rendre sa détection difficile. A titre d'exemple non-limitatif, une opération factice peut être l'exécution réelle d'un calcul, mais sans enregistrement du résultat en mémoire, ou avec enregistrement, mais dans une mémoire inopérante pour l'opération considérée.

Les opérations factices permettent ainsi d'introduire de faux calculs, ou de faux sous-ensembles d'opérations.

La présente invention concerne également un dispositif électronique d'exécution d'un algorithme, par exemple une carte à puce, caractérisé en ce qu'il met en oeuvre le procédé de sécurisation précité, éventuellement avec les aspects optionnels qui sont décrits dans ce qui suit.

Les différents aspects et avantages de l'invention apparaîtront plus clairement dans la suite de la description, qui présente un exemple de mise en oeuvre préféré du procédé selon l'invention et qui n'est donné qu'à titre indicatif et nullement limitatif de l'invention.

Selon un mode préféré de l'invention, un certain nombre d'opérations factices sont insérées entre des opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Ces opérations factices sont introduites de

façon aléatoire : ces opérations factices peuvent être introduites entre n'importe quelle opération utile associée à l'algorithme.

On peut également trouver une ou plusieurs opérations factices avant la première opération utile associée à un algorithme ou après la dernière opération utile associée à un algorithme. On peut également trouver plusieurs opérations factices consécutives.

Afin de donner des séries de mesure de courant différentes à chaque exécution d'un même algorithme, de nouveaux aléas sont introduits à chaque exécution d'un algorithme.

Néanmoins, dans une application préférée, le procédé selon l'invention comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations, qu'elles soient utiles et/ou factices successives. Ainsi, l'insertion des opérations factices n'apparaît pas de façon évidente lors d'une étude temporelle des signaux électriques associés aux opérations utiles réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Enfin, il est préférable, mais pas obligatoire, que le nombre d'opérations factices introduites dans l'enchaînement d'opérations utiles soit constant pour chaque nouvelle exécution de l'algorithme. Ainsi, le temps d'exécution de l'algorithme dans sa totalité est le même à chaque exécution de l'algorithme. Le fait que des opérations factices ont été introduites est ainsi invisible en première analyse, ce qui assure encore une meilleure sécurisation de l'enchaînement d'opérations utiles.

Selon l'invention, il est également possible de distribuer les aléas seulement sur certaines parties de l'algorithme. De plus, le procédé selon l'invention

peut également s'appliquer à des algorithmes dont les opérations sont ordonnées, c'est-à-dire que les opérations utiles doivent s'enchaîner dans un ordre qu'on ne peut pas changer.

Le nombre d'opérations factices introduites est, dans une application préférée de l'invention, de l'ordre de 2 pourcent sur le nombre total d'opérations effectuées.

REVENDICATIONS

1. Procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations.

2. Procédé de sécurisation d'un enchaînement d'opérations de même type selon la revendication 1, caractérisé en ce que le procédé comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations utiles et/ou factices successives.

3. Procédé de sécurisation d'un enchaînement d'opérations de même type selon l'une des revendications 1 ou 2, caractérisé en ce que le nombre d'opérations factices introduites dans l'enchaînement d'opérations est constant pour chaque nouvelle exécution de l'algorithme.

4. Utilisation du procédé selon l'une des revendications précédentes dans le domaine de la cryptographie.

5. Dispositif électronique d'exécution d'un algorithme, caractérisé en ce qu'il met en oeuvre le procédé de sécurisation selon l'une quelconque des revendications 1 à 3.

6. Carte à puce comprenant un dispositif électronique d'exécution d'un algorithme, caractérisé en ce qu'il met en oeuvre le procédé de sécurisation selon l'une quelconque des revendications 1 à 3.